Améliorez la performance et la sécurité de votre WAN

Cisco Catalyst SD-WAN

Nicolas Boursier – Solutions Engineer
Vincent Redon – Solutions Engineer
Track 3 - Session 3

Agenda

- Update marché
- Comment améliorer la résilience de l’infrastructure avec Catalyst SD-WAN Security?
- AIOps pour Catalyst SD-WAN
- Conclusion

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Update marché

Trends shaping the transformation of WAN Edge

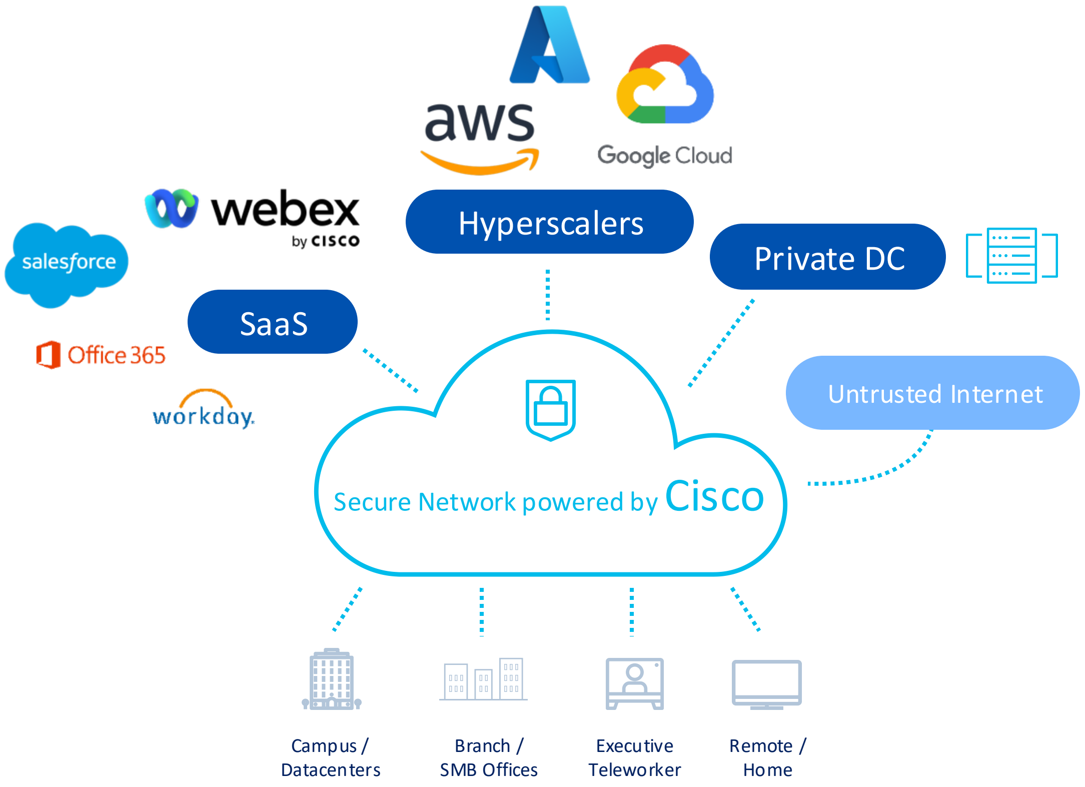
Internet-only branch ➔ Shifting to a Security By Design mindset

Apps moving to SaaS & IaaS ➔ Multicloud acceleration

Keep control over distributed infrastructure ➔ Digital experience monitoring/assurance

Simplify IT ➔ Centralized management distributed enforcement

Reduce Footprint/Sustainability ➔ multiple network function in one box



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Customers' SD-WAN asks

Hidden
Not public information

Security

But not just security !

Other keep requirements

Application performance management
ML/AI tools
Robust centralized orchestration
Complete Cloud integration
Scalability

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Hidden
Not public information

Does SASE make SD-WAN Obsolete?

Hidden
Not public information

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Is SD-WAN still needed in UZTNA ?

Hidden
Not public information

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reality behind UZTNA

Hidden
Not public information

User Experience

- ➔ How to improve WAN usage and performance?
- ➔ How to provide SaaS acceleration?
- ➔ How to optimize SSE reachability
- ➔ End-to-end Observability required

- ➔ Need agentless solution for connections to SSE (IPsec VPN)

Insider attacks

- ➔ Need East-West segmentation

Cloud to Cloud security

- ➔ Need East-West segmentation

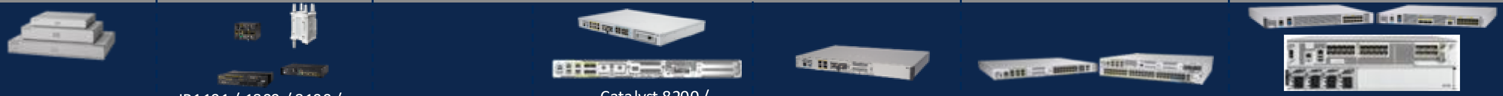
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Comment améliorer la résilience de l'infrastructure avec Catalyst SD-WAN Security

Introducing the Catalyst SD-WAN Adaptive Security

Catalyst SD-WAN

Threat Intelligence | Zero Trust | Simplified Workflows | Security Insights | Granular Controls | Technology Alliances



ISR 1000

IR1101 / 1800 / 8100 / 8300 / ESR 6300

Catalyst 8000V

Catalyst 8200 / C8300-uCPE **

Catalyst 8200, 8200L

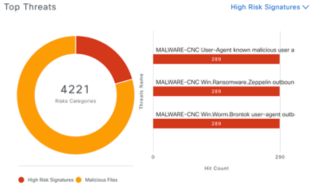
Catalyst 8300

Catalyst 8500, 8500L

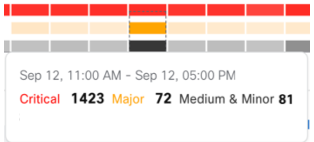
3 Monitoring & Visibility

Cisco on Cisco

SecOps Persona | Security Insights | Customized Dashboard


Top Threats
High Risk Signatures
4221
Risks Categories
Threats Name
MALWARE-CNC User-Agent known malicious user a
289
MALWARE-CNC Win.Ransomware.Zeppelin outboun
289
MALWARE-CNC Win.Worm.Brontok user-agent outb
289
0
290
Hit Count
High Risk Signatures
Malicious Files

Security Heatmap | Alarms | Security Events | Real-Time Updates



Sep 12, 11:00 AM - Sep 12, 05:00 PM

Critical **1423** Major **72** Medium & Minor **81**

SIEM/SOAR

splunk>

Microsoft Sentinel

Network & Cloud Security

1 on-box NGFW

Embedded Security Stack

No External Firewall Required

Powered by Cisco Talos

Reliable | Scalable | Flexible

- Application firewall
- Intrusion Prevention System (IPS)
- Advanced Malware Protection
- URL Filtering
- **Live** Signature Updates
- Unified Logging
- Segmentation
- TLS Decryption
- Sandboxing
- DNS-layer security
- Cisco ISE Integration
- Dynamic Core Allocation

2 Cloud Security Integration (SSE)

Cisco on Cisco

Unified SASE | Automation | Comprehensive Security

Cisco Umbrella

Cisco Secure Access

SASE

SD-WAN + SSE

SSE Technology Alliance

3rd Party SSE Integration | Integrated SASE

zscaler

paloalto networks

Skyhigh Security

CLOUDFLARE

netskope

- Simplified Configuration
- Multi-Tunnel Automation Enhanced throughput using 8 tunnels
- Active/Standby Tunnels
- Traffic Load Balancing
- Layer-7 Health Check
- Optimized SaaS
- Service Resiliency (DC fallback option)

4 Certification

Industry Certifications

- PCI-DSS
- SOC2/SOC3
- 27001, 27017 27018, 27701
- C5
- FIPS 140-2
- FedRAMP **

** In progress

5 Fabric Security

Encrypted Security Keys

- Encrypted Control Plane
- Encrypted Data Plane
- HW Based Device Authentication (SUDI)
- Enhanced Security Pairwise Keys
- DDoS Protection

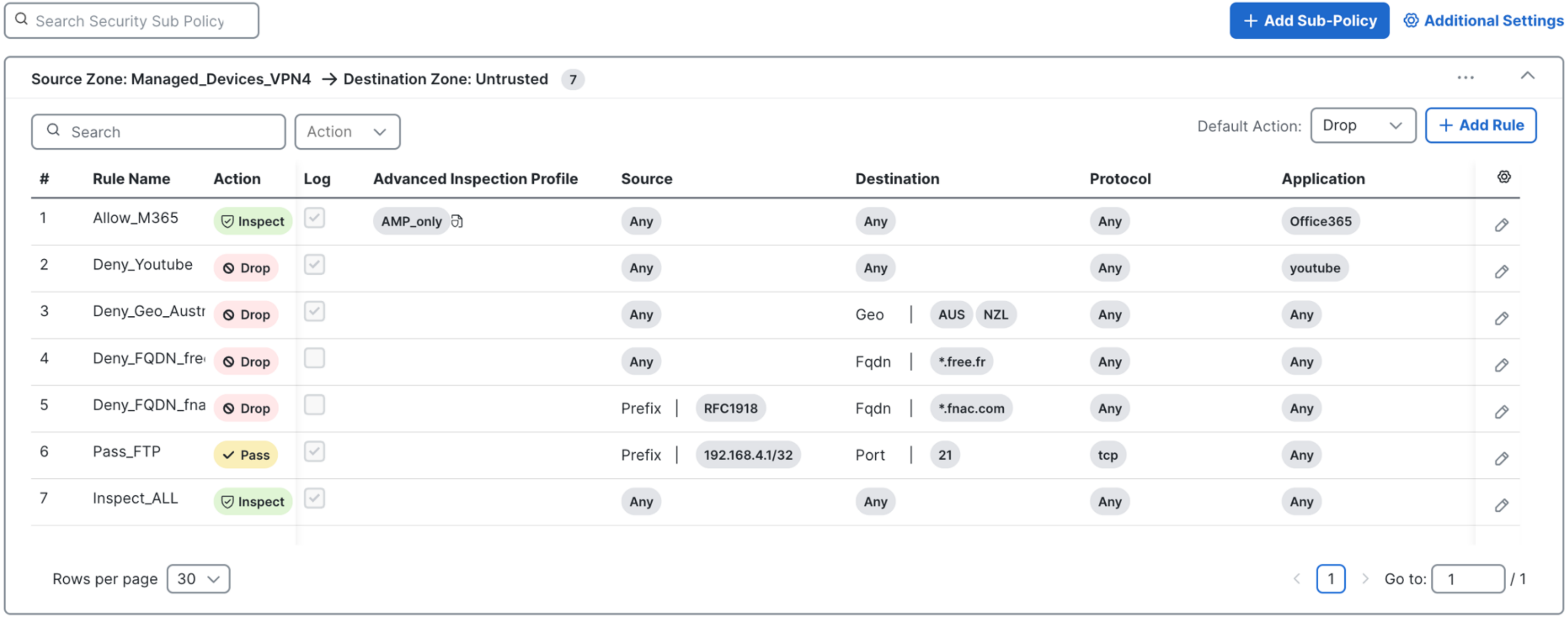
cisco Connect

#CiscoConnect

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

On-Box NGFW

Catalyst Firewall Rule Expert View



Source Zone: Managed_Devices_VPN4 → Destination Zone: Untrusted 7

Default Action: Drop

#	Rule Name	Action	Log	Advanced Inspection Profile	Source	Destination	Protocol	Application
1	Allow_M365	Inspect	☑	AMP_only	Any	Any	Any	Office365
2	Deny_Youtube	Drop	☑		Any	Any	Any	youtube
3	Deny_Geo_Austr	Drop	☑		Any	Geo | AUS NZL	Any	Any
4	Deny_FQDN_fre	Drop	☐		Any	Fqdn | *.free.fr	Any	Any
5	Deny_FQDN_fna	Drop	☐		Prefix | RFC1918	Fqdn | *.fnac.com	Any	Any
6	Pass_FTP	Pass	☑		Prefix | 192.168.4.1/32	Port | 21	tcp	Any
7	Inspect_ALL	Inspect	☑		Any	Any	Any	Any

Rows per page 30

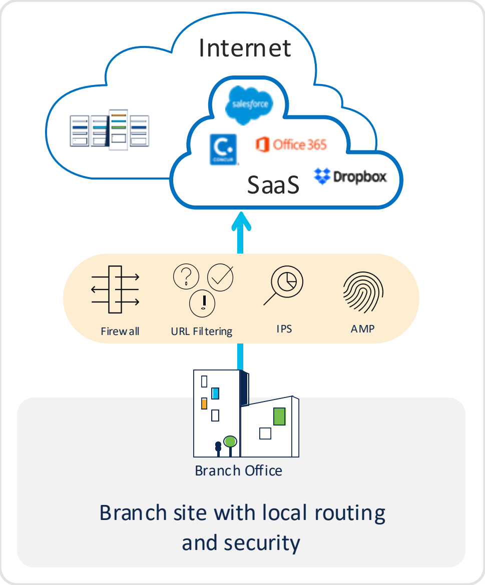
Go to: 1 / 1

Comprehensive view of FW rule table allowing the SOC to easily search all elements of FW rules and edit

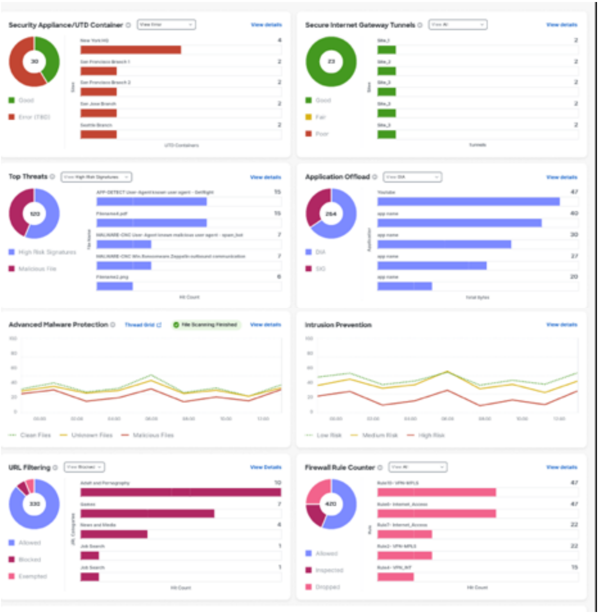
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

On-Box NGFW

Centralized management of advanced security



Branch site with local routing and security


Security Appliance/UTD Container
Secure Internet Gateway Tunnels
Top Threats
Application Offload
Advanced Malware Protection
Intrusion Prevention
URL Filtering
Firewall Rule Counter

Next Gen Firewall (NGFW)

Guided workflows

Unified management

See It all, manage It all

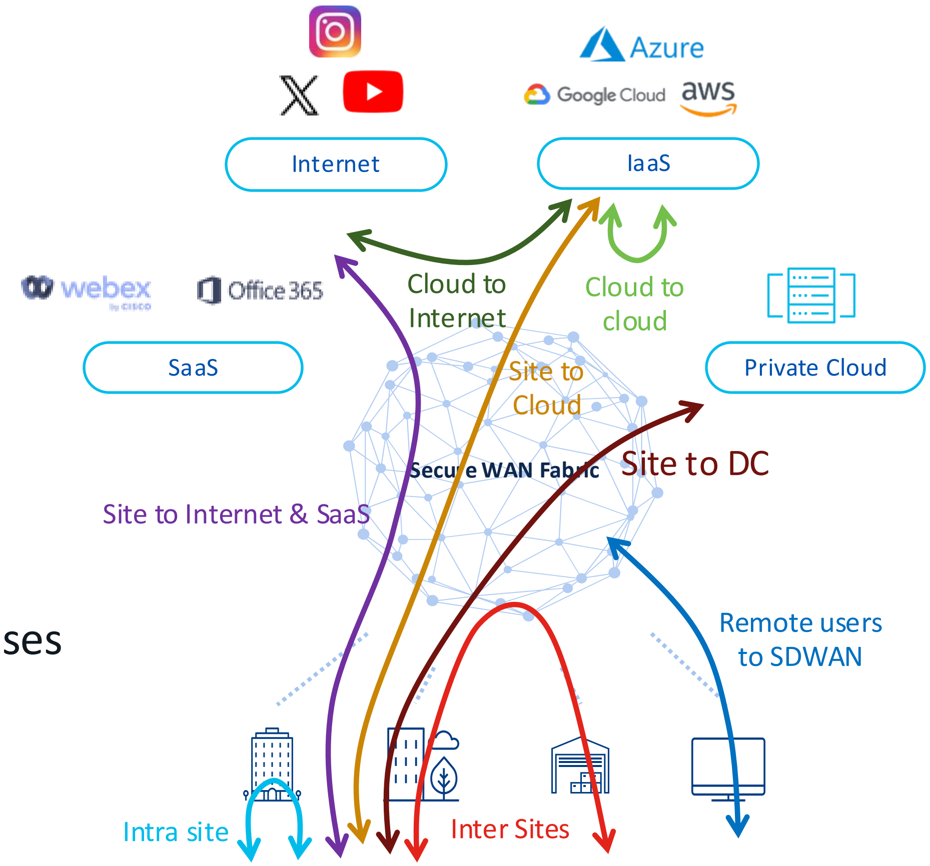
Reduce security cost

Unleash faster apps

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use cases

Consistent security policies across uses cases



Internet

IaaS

SaaS

Private Cloud

Cloud to Internet

Cloud to cloud

Site to Cloud

Secure WAN Fabric

Site to DC

Site to Internet & SaaS

Remote users to SDWAN

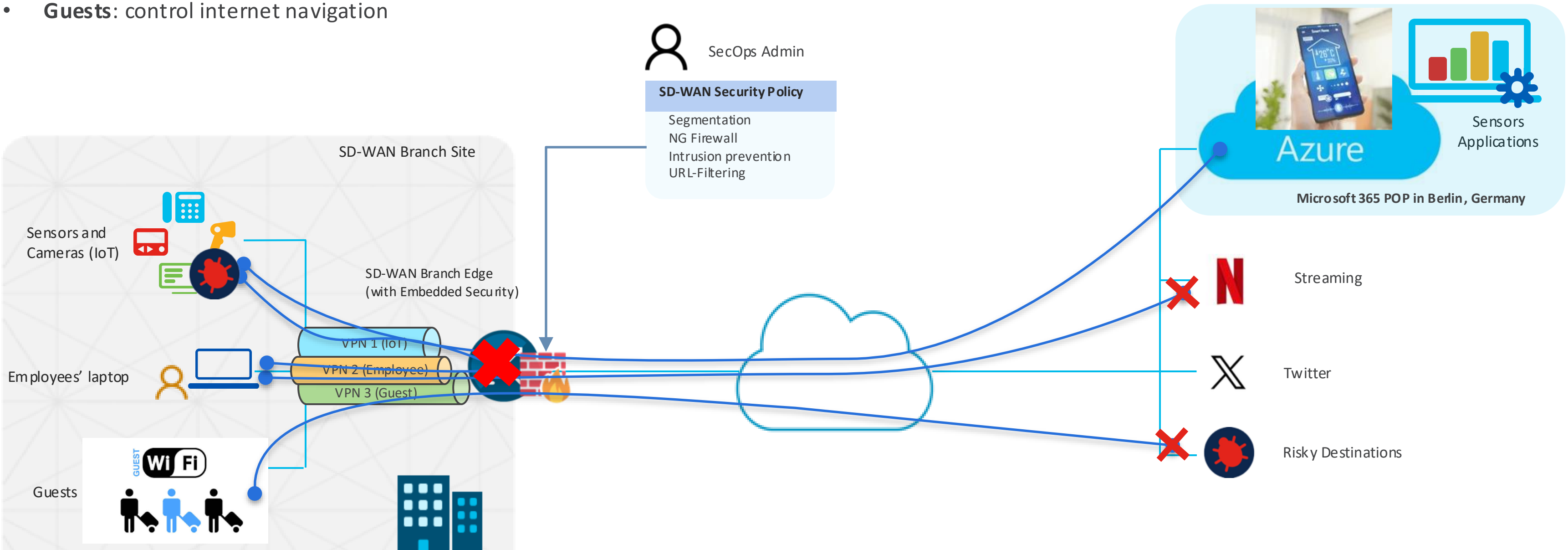
Intra site

Inter Sites

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

[North-South] Branch - Direct Internet Access Security enforcement

- **IoT** : Control internet destination and traffic behavior on
- **Employees**: allow internet access but avoid risky destination and high throughput internet services
- **Guests**: control internet navigation



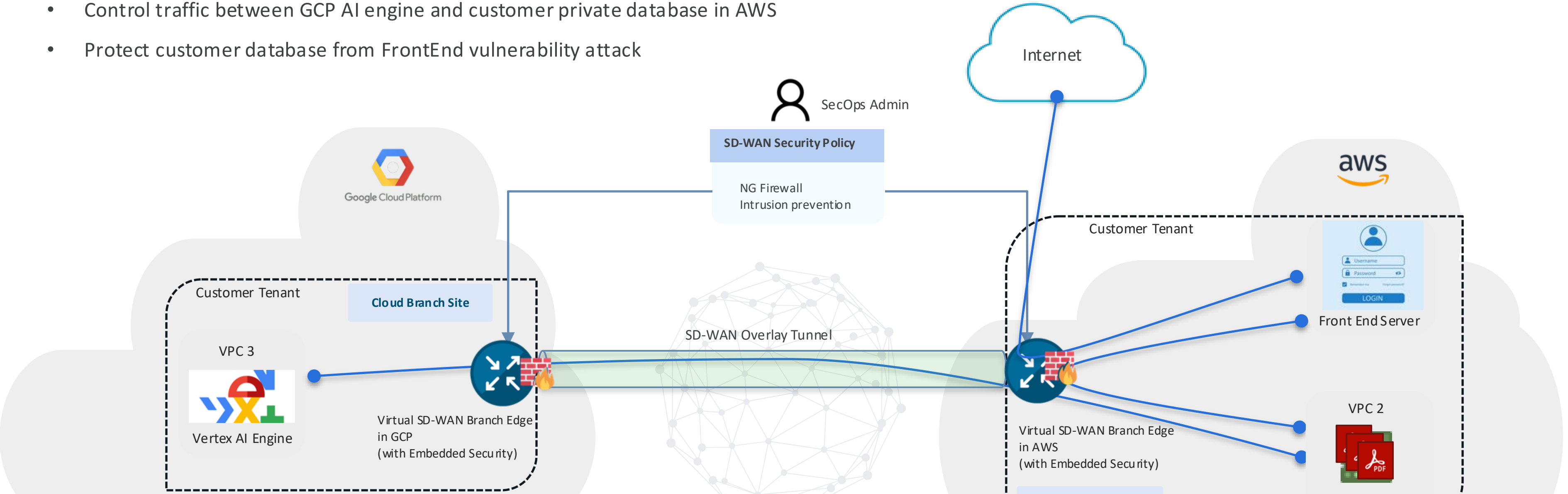
SD-WAN Security Policy

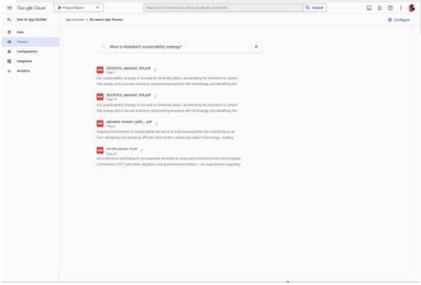
Source	Inspect	Block	Exempt	Advanced Inspection Profile
Sensors	Azure Berlin tenant	All other destinations	None	
Employees (IT)	All DIA Traffic	Streaming Media, P2P, Risky destinations	Internal domains	URL-F
Guest Wi-fi	All DIA Traffic	Social Media, risky destinations	Twitter	URL-F, IPS

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

[East-West] Cloud to Cloud security enforcement

- Control traffic between GCP AI engine and customer private database in AWS
- Protect customer database from FrontEnd vulnerability attack





SD-WAN

Security Policy

Source	Allow	Deny	Advanced Inspection Profile
Internet users	Front End Server (Port# 443)	All	IPS
Front End Server	Database Server (Port# 1433 - SQL)	All	IPS
Vertex AI Engine	Database Server (Port# 443)	All	

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco's Universal Zero Trust Network Access

All kinds of users

All kinds of workplaces

Managed and unmanaged devices

All kinds of things (IT/IOT)s

Universal ZTNA

Public SaaS apps

Web

Modern/ZTNA private apps

Legacy private apps

Gen AI apps

Converged network and security

New items

Flexible Enforcement

Enterprise browser integration

Guardrails for AI use

Policy Assurance

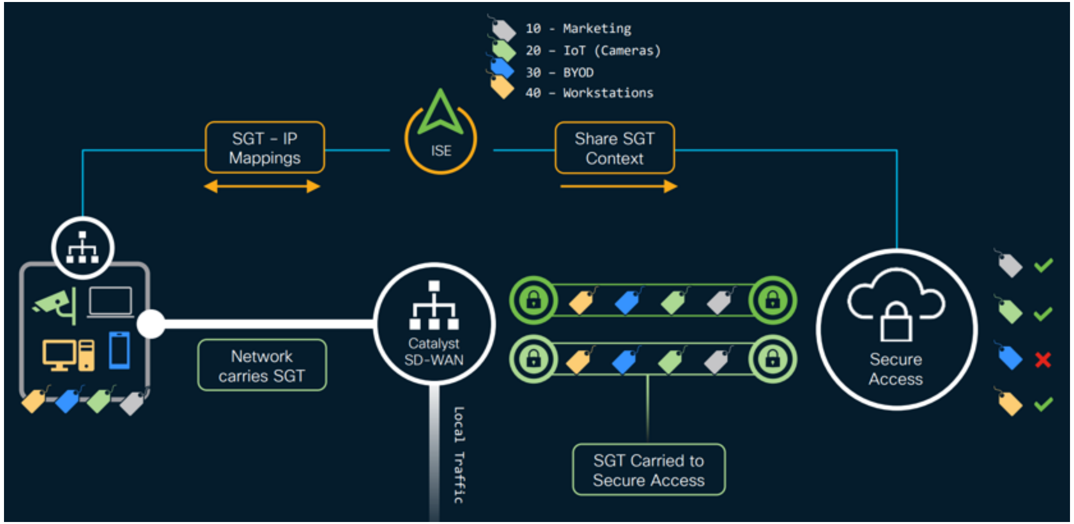
Enforce zero trust using Identity Context

Consistent network micro-segmentation - End to End
SGT Support for consistent policy enforcement

Uniquely identify devices and traffic based on context from ISE

SGT Based Policy across network and Cloud

Maintain micro segmentation through Secure Access

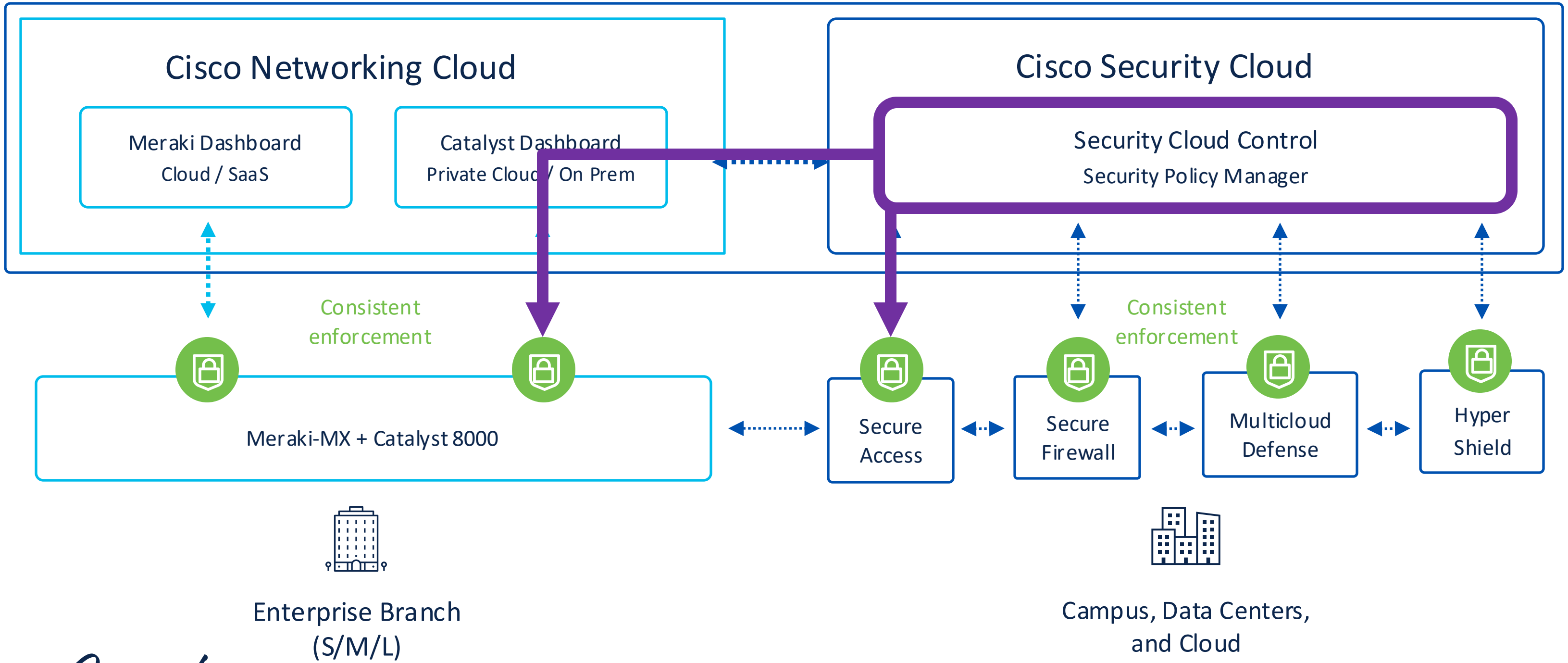


#CiscoConnect

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unified Secure WAN experience

Centralized security policy with consistent enforcement at WAN Edge irrespective of the location



Cisco Networking Cloud

Meraki Dashboard
Cloud / SaaS

Catalyst Dashboard
Private Cloud / On Prem

Cisco Security Cloud

Security Cloud Control
Security Policy Manager

Consistent enforcement

Meraki-MX + Catalyst 8000

Consistent enforcement

Secure Access

Secure Firewall

Multicloud Defense

Hyper Shield

Enterprise Branch
(S/M/L)

Campus, Data Centers, and Cloud

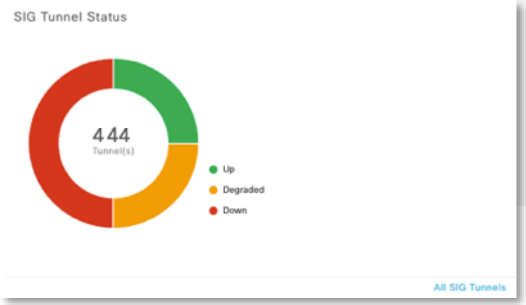
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

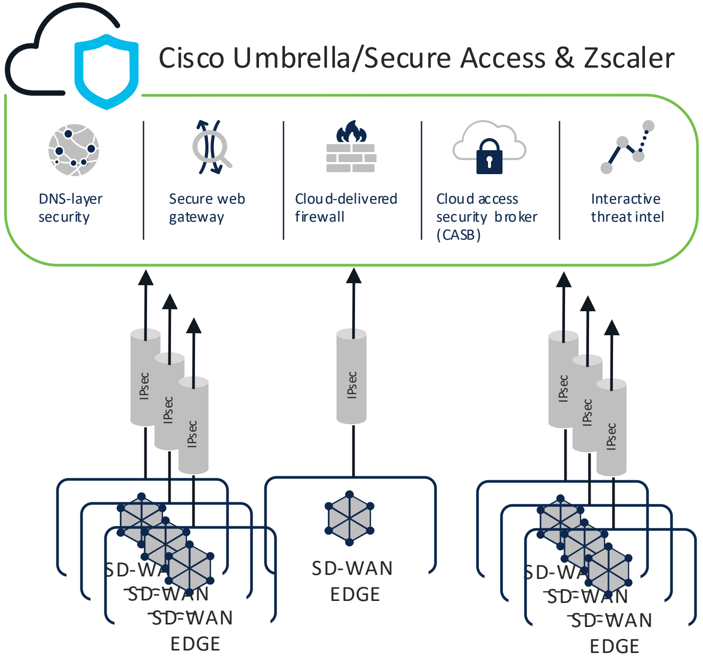
Simplified SASE Deployment and Monitoring

Automated tunnel deployment

Automated HA Design

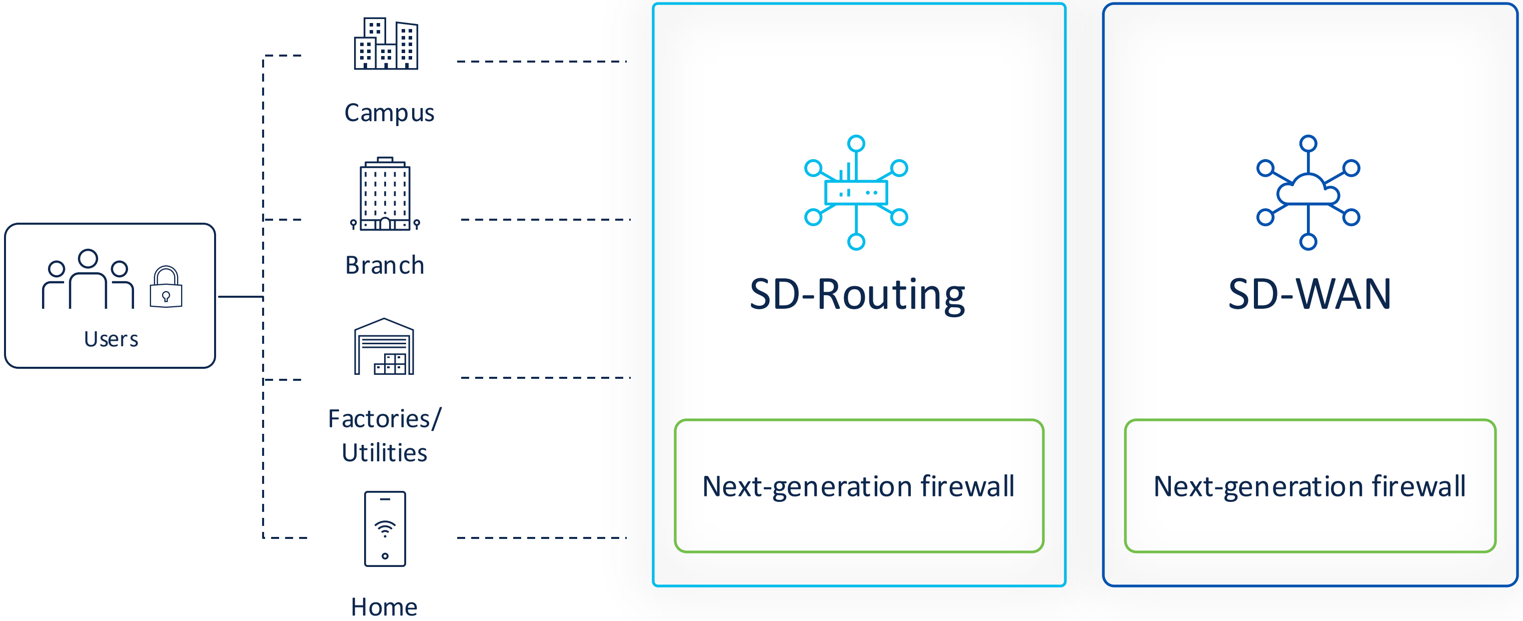
Tunnel performances monitoring


SIG Tunnel Status


Cisco Umbrella/Secure Access & Zscaler

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure WAN



Users

Campus

Branch

Factories/ Utilities

Home

SD-Routing

Next-generation firewall

SD-WAN

Next-generation firewall

ISR 1000

IR

Catalyst 8000V

Catalyst 8200 / C8300-uCPE**

Catalyst 8200, 8200L

Catalyst 8300

Catalyst 8500, 8500L

#CiscoConnect

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

AIOps for Catalyst SD-WAN

A quoi sert l’IA dans un contexte SD-WAN?

- Analyser les nombreuses données de métrologie générées au sein d’une fabrique SD-WAN

- Faire des prédictions et des recommandations

- Identifier les problèmes avant qu’ils ne deviennent critiques

- Interagir avec un assistant IA en langage naturel afin d’obtenir plus simplement et rapidement les informations souhaitées

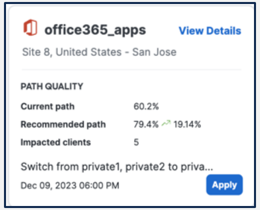
➢ Bénéfices:
  - Améliorer l’expérience utilisateur
  - Efficacité opérationnelle

AIOps: Improve user experience and simplify operations

Improve user experience

Simplify operations

Predictive Path Recommendations



office365_apps View Details

Site 8, United States - San Jose

PATH QUALITY

Current path	60.2%
Recommended path	79.4% ↗ 19.14%
Impacted clients	5

Switch from private1, private2 to priva...

Dec 09, 2023 06:00 PM

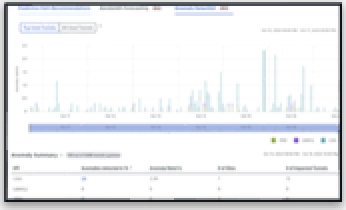
Path recommendations to Improve Application Performance

Bandwidth Forecasting

AI/ML-based forecasting

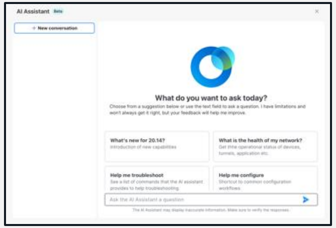
Capacity planning

Anomaly Detection



Detect Network Anomalies

AI Assistant for Networking



What do you want to ask today?

Choose from a suggestion below or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

What's new for 20.14?
Introduction of new capabilities

What is the health of my network?
Get the operational status of devices, tunnels, application etc.

Help me troubleshoot
See a list of commands that the AI assistant provides to help troubleshooting.

Help me configure
Shortcut to common configuration workflows.

Ask the AI Assistant a question

The AI Assistant may display inaccurate information. Make sure to verify the responses.

Interactive LLM-based AI Assistant for Networking (Gen AI)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Predictive Path Recommendations

Predictive Path Recommendations

Powered by ThousandEyes WAN Insights

Forecast issues and make policy recommendations

1. Collect Telemetry

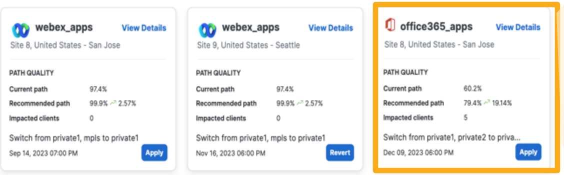
Collect network telemetry via SD-WAN Analytics

2. Data Analysis

Predictive modeling to forecast issues & make path recommendations

3. Apply Recommendations

Fine-tune SD-WAN policies to make path changes to improve App experience

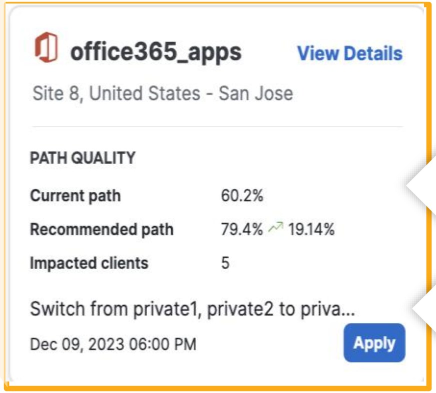


webex_apps
Site 8, United States - San Jose
PATH QUALITY
Current path 97.4%
Recommended path 99.9% 2.57%
Impacted clients 0
Switch from private1, mpls to private1
Sep 14, 2023 07:00 PM

webex_apps
Site 9, United States - Seattle
PATH QUALITY
Current path 97.4%
Recommended path 99.9% 2.57%
Impacted clients 0
Switch from private1, mpls to private1
Nov 16, 2023 06:00 PM

office365_apps
Site 8, United States - San Jose
PATH QUALITY
Current path 60.2%
Recommended path 79.4% 19.14%
Impacted clients 5
Switch from private1, private2 to priva...
Dec 09, 2023 06:00 PM

Transforming IT operations from a reactive to a predictive model



office365_apps
Site 8, United States - San Jose
PATH QUALITY
Current path 60.2%
Recommended path 79.4% 19.14%
Impacted clients 5
Switch from private1, private2 to priva...
Dec 09, 2023 06:00 PM

Current & Recommended Path Quality with estimated % gain

Recommends the path to switch to

Out-of-the-box Application Groups

Office 365 Webex Google Workspace Salesforce GoTo Meeting Voice

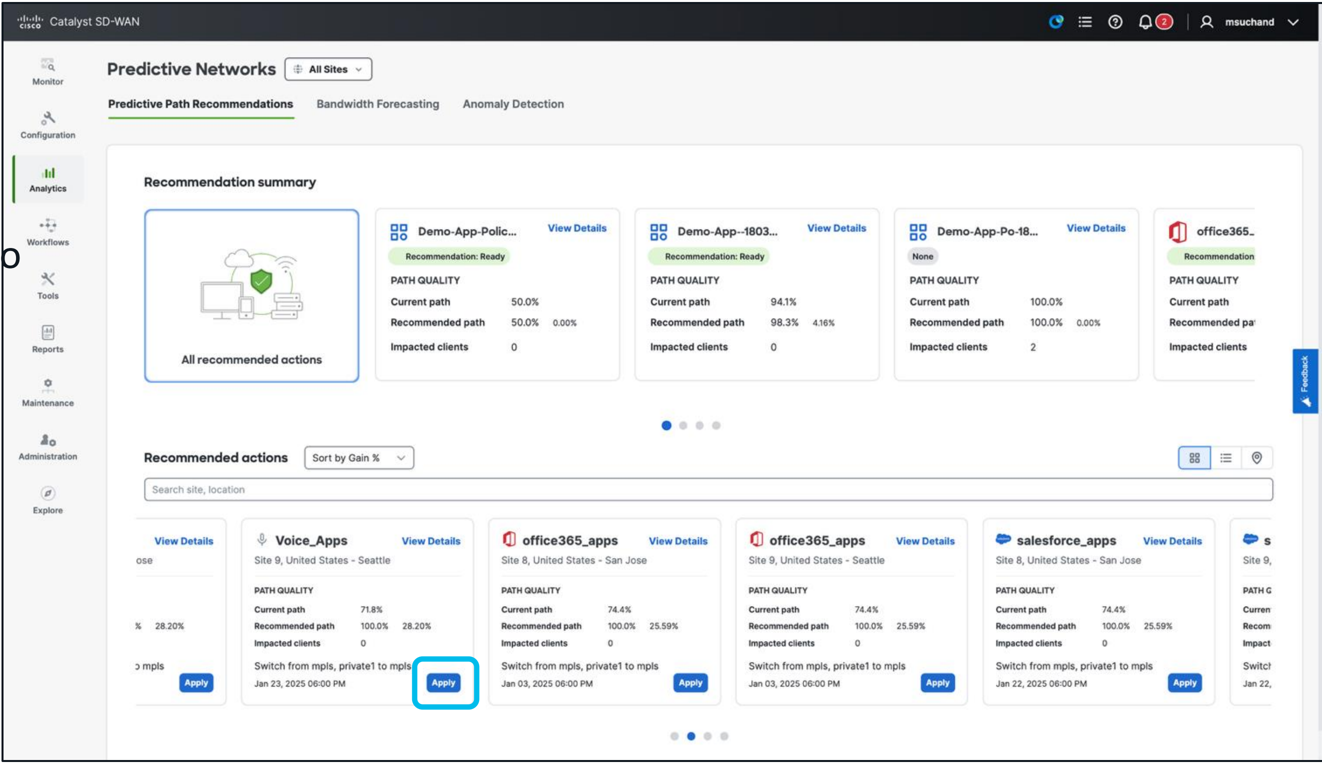
- Included with SD-WAN DNA Advantage+ license; ThousandEyes Enterprise Agent not necessary

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Predictive Path Recommendations

Landing page, Recommendation summary, Recommended actions

- Review Recommendation summary by Application Group
- Click on an Application Group to view more details
- Per site recommendations across the Network



Recommendation summary

Demo-App-Polic... — Recommendation: Ready
PATH QUALITY
Current path 50.0%
Recommended path 50.0% 0.00%
Impacted clients 0

Demo-App--1803... — Recommendation: Ready
PATH QUALITY
Current path 94.1%
Recommended path 98.3% 4.16%
Impacted clients 0

Demo-App-Po-18... — None
PATH QUALITY
Current path 100.0%
Recommended path 100.0% 0.00%
Impacted clients 2

Recommended actions

Voice_Apps — Site 9, United States - Seattle
PATH QUALITY
Current path 71.8%
Recommended path 100.0% 28.20%
Impacted clients 0
Switch from mpls, private1 to mpls
Jan 23, 2025 06:00 PM

office365_apps — Site 8, United States - San Jose
PATH QUALITY
Current path 74.4%
Recommended path 100.0% 25.59%
Impacted clients 0
Switch from mpls, private1 to mpls
Jan 03, 2025 06:00 PM

office365_apps — Site 9, United States - Seattle
PATH QUALITY
Current path 74.4%
Recommended path 100.0% 25.59%
Impacted clients 0
Switch from mpls, private1 to mpls
Jan 03, 2025 06:00 PM

salesforce_apps — Site 8, United States - San Jose
PATH QUALITY
Current path 74.4%
Recommended path 100.0% 25.59%
Impacted clients 0
Switch from mpls, private1 to mpls
Jan 22, 2025 06:00 PM

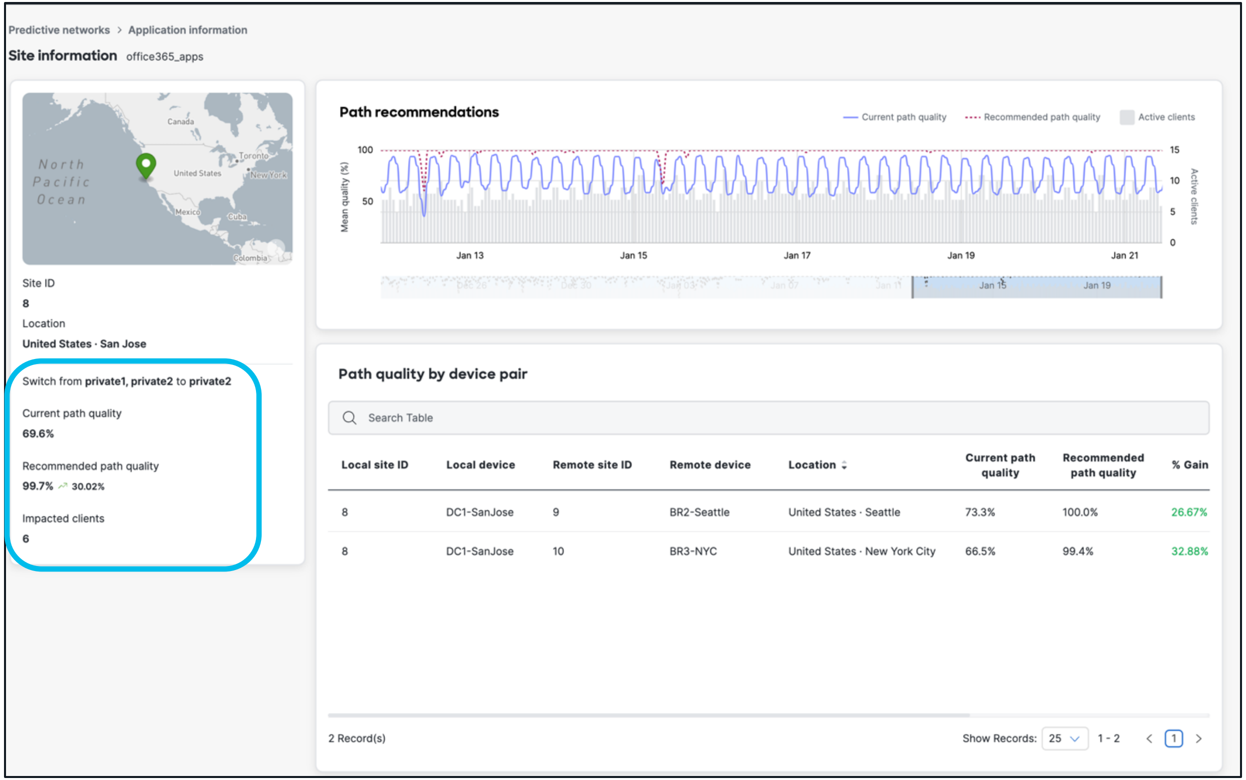
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Predictive Path Recommendations

Recommendation details

- Recommendation for **Office365_apps** on DC1-San-Jose site:

➔ Switch the traffic to “private2” instead of load balancing between private1 & private2 paths



Predictive networks > Application information

Site information office365_apps

Site ID
8

Location
United States · San Jose

Switch from **private1, private2** to **private2**

Current path quality
69.6%

Recommended path quality
99.7% 30.02%

Impacted clients
6

Path recommendations

Path quality by device pair

Search Table

Local site ID	Local device	Remote site ID	Remote device	Location	Current path quality	Recommended path quality	% Gain
8	DC1-SanJose	9	BR2-Seattle	United States · Seattle	73.3%	100.0%	26.67%
8	DC1-SanJose	10	BR3-NYC	United States · New York City	66.5%	99.4%	32.88%

2 Record(s)

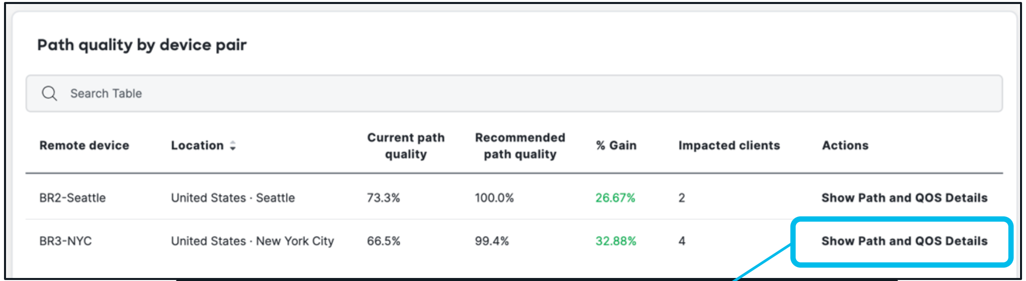
Show Records: 25 1 - 2 < 1 >

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Predictive Path Recommendations

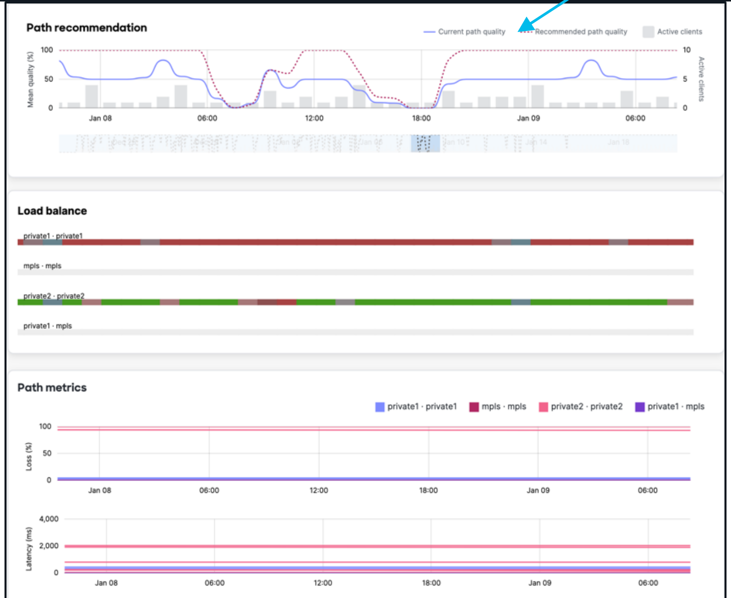
Path and QoS details

- Graphs showing default & recommended path quality between selected device pair
- Color-coded lines reflecting quality of network paths between selected pair
    - Also includes line charts showing loss, latency and jitter over these paths


Path quality by device pair

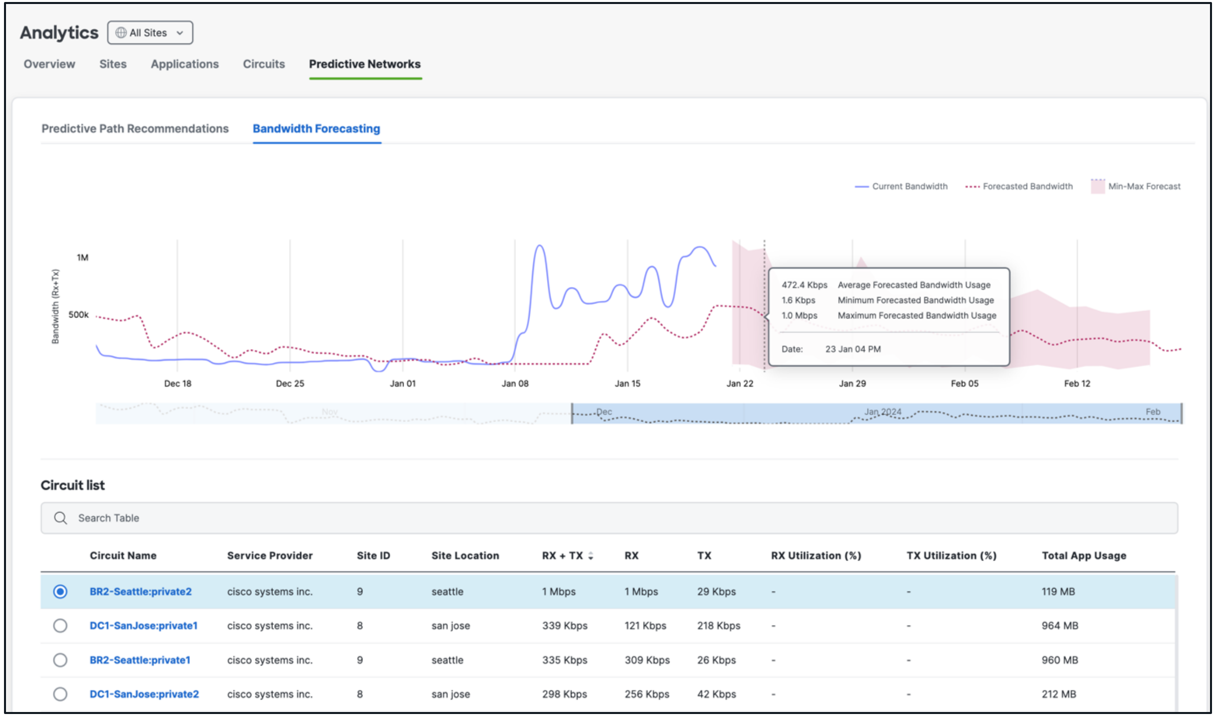
Search Table

Remote device	Location	Current path quality	Recommended path quality	% Gain	Impacted clients	Actions
BR2-Seattle	United States · Seattle	73.3%	100.0%	26.67%	2	Show Path and QOS Details
BR3-NYC	United States · New York City	66.5%	99.4%	32.88%	4	Show Path and QOS Details



Bandwidth Forecasting

AIOps: Bandwidth Forecasting



472.4 Kbps	Average Forecasted Bandwidth Usage
1.6 Kbps	Minimum Forecasted Bandwidth Usage
1.0 Mbps	Maximum Forecasted Bandwidth Usage

Date: 23 Jan 04 PM

Circuit list

Search Table

	Circuit Name	Service Provider	Site ID	Site Location	RX + TX	RX	TX	RX Utilization (%)	TX Utilization (%)	Total App Usage
●	BR2-Seattle:private2	cisco systems inc.	9	seattle	1 Mbps	1 Mbps	29 Kbps	-	-	119 MB
○	DC1-SanJose:private1	cisco systems inc.	8	san jose	339 Kbps	121 Kbps	218 Kbps	-	-	964 MB
○	BR2-Seattle:private1	cisco systems inc.	9	seattle	335 Kbps	309 Kbps	26 Kbps	-	-	960 MB
○	DC1-SanJose:private2	cisco systems inc.	8	san jose	298 Kbps	256 Kbps	42 Kbps	-	-	212 MB

Benefits

Helps organizations with capacity planning.

Identify Growth Trends, Visualize Seasonality & Surges in Circuit Usage.

Highlights

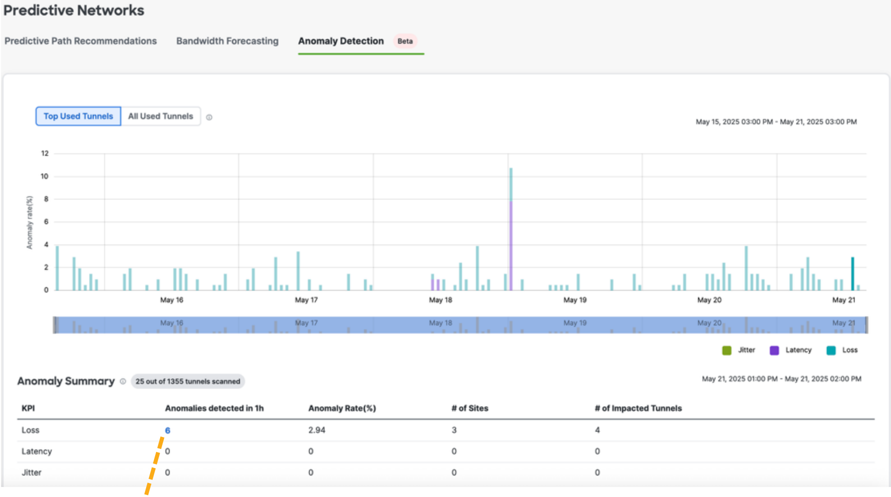
- Track historical usage of individual circuits and forecast future usage (Top 50 circuits)
- Provide 12 weeks forecast based on statistical models and ML technique
- Train the AI model by comparing historical bandwidth usage from the 52 last weeks to forecast bandwidth usage

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Anomaly Detection

Available in Beta

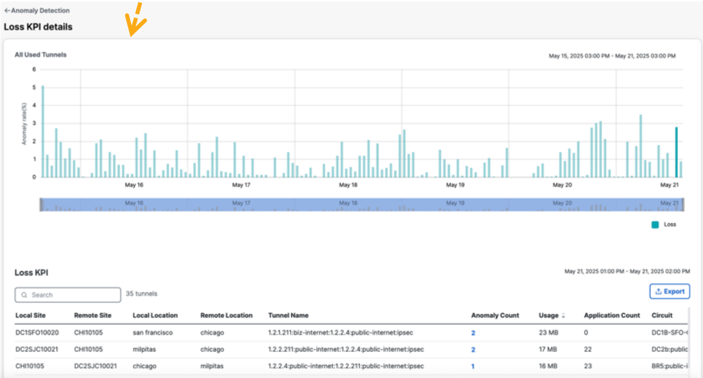
Anomaly Detection



Anomaly Summary 25 out of 1355 tunnels scanned

May 21, 2025 01:00 PM - May 21, 2025 02:00 PM

KPI	Anomalies detected in 1h	Anomaly Rate(%)	# of Sites	# of Impacted Tunnels
Loss	6	2.94	3	4
Latency	0	0	0	0
Jitter	0	0	0	0



Loss KPI 35 tunnels

May 21, 2025 01:00 PM - May 21, 2025 02:00 PM

Local Site	Remote Site	Local Location	Remote Location	Tunnel Name	Anomaly Count	Usage	Application Count	Circuit
DC1SFO10020	CHI10105	san francisco	chicago	1.2.1.211:biz-internet:1.2.2.4:public-internet:ipsec	2	23 MB	0	DC1B-SFO-
DC2SJC10021	CHI10105	milpitas	chicago	1.2.2.211:public-internet:1.2.2.4:public-internet:ipsec	2	17 MB	22	DC2b:public
CHI10105	DC2SJC10021	chicago	milpitas	1.2.2.4:public-internet:1.2.2.211:public-internet:ipsec	1	16 MB	23	BR5:public-i

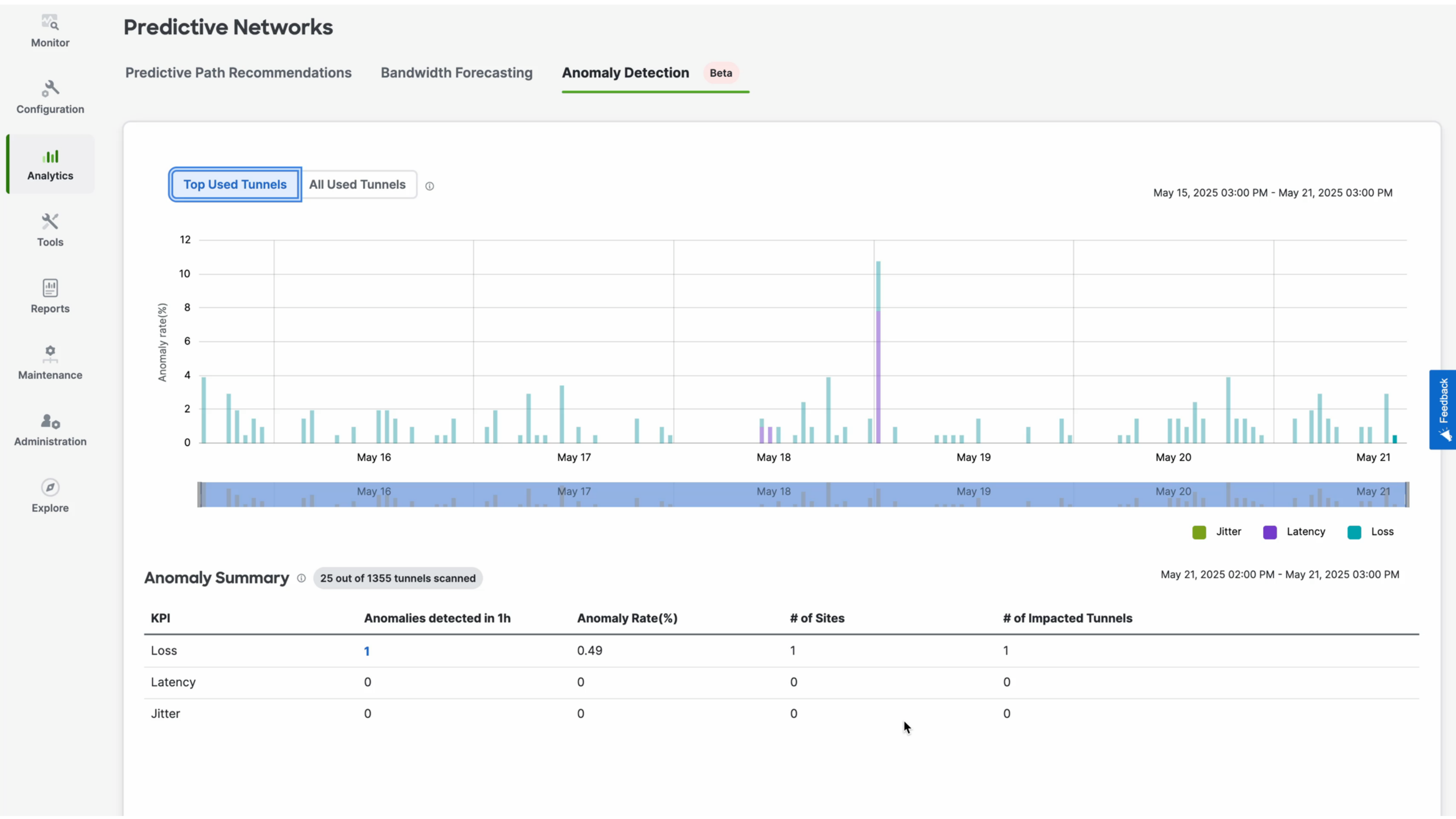
Highlights

- ✓ Identify tunnels with anomalies across key network KPIs (loss, latency, jitter)
- ✓ Determine impact radius based on site count, usage & app count
- ✓ Determine if it's a chronic issue by viewing the trend information

Benefits

- ✓ Early problem detection: Identify unusual patterns before they manifest into larger issues
- ✓ Improve operational efficiency: Streamline operations & reduce downtime
- ✓ Optimize network performance: Fine-tune your network to improve end-user experience

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Predictive Networks

May 15, 2025 03:00 PM - May 21, 2025 03:00 PM

Anomaly Summary

25 out of 1355 tunnels scanned

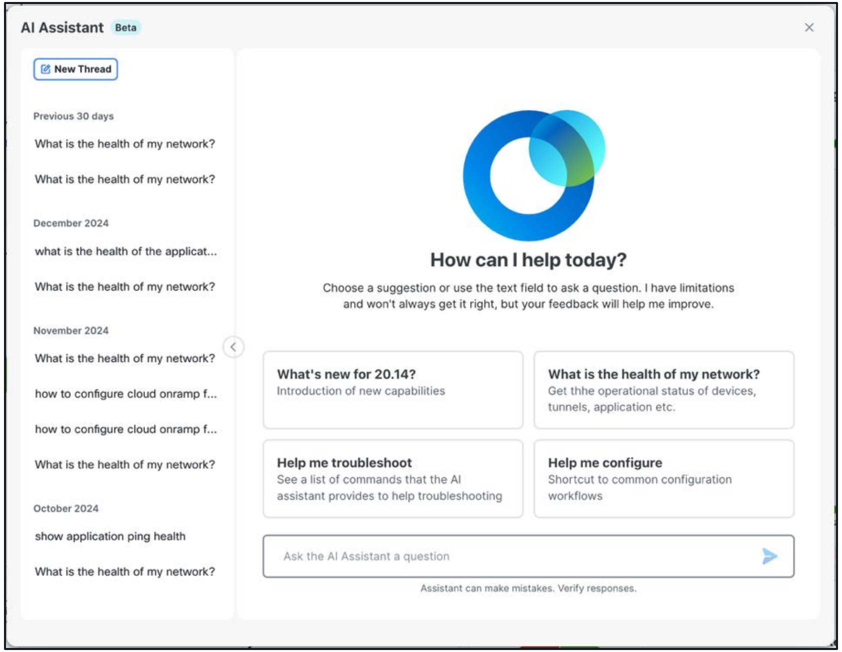
May 21, 2025 02:00 PM - May 21, 2025 03:00 PM

KPI	Anomalies detected in 1h	Anomaly Rate(%)	# of Sites	# of Impacted Tunnels
Loss	1	0.49	1	1
Latency	0	0	0	0
Jitter	0	0	0	0

AI Assistant for Networking

AIOps: AI Assistant for Networking

Available in Beta



Previous 30 days

What is the health of my network?

What is the health of my network?

December 2024

what is the health of the applicat...

What is the health of my network?

November 2024

What is the health of my network?

how to configure cloud onramp f...

how to configure cloud onramp f...

What is the health of my network?

October 2024

show application ping health

What is the health of my network?

How can I help today?

Choose a suggestion or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

What's new for 20.14?
Introduction of new capabilities

What is the health of my network?
Get thhe operational status of devices, tunnels, application etc.

Help me troubleshoot
See a list of commands that the AI assistant provides to help troubleshooting

Help me configure
Shortcut to common configuration workflows

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.

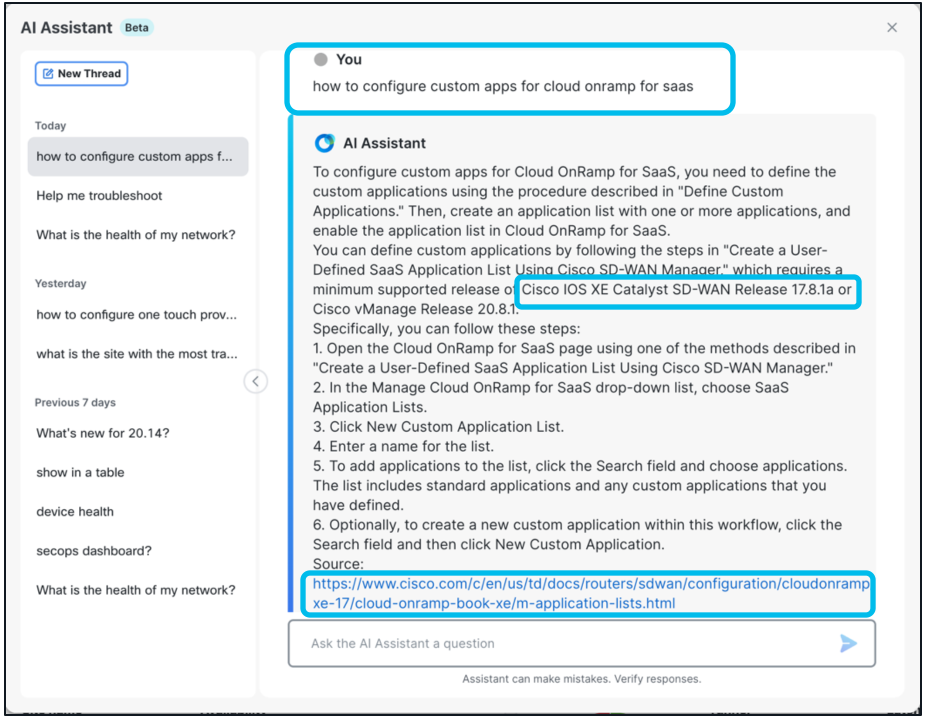
Benefits

- Interactive LLM-based AI Assistant
- Help with **feature-related user queries** w/ information fetched from documentation
- Help with **operational queries**, such as health information

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

AI Assistant for Networking

Use Case: Knowledge Fetch


AI Assistant Beta
New Thread
Today
how to configure custom apps f...
Help me troubleshoot
What is the health of my network?
Yesterday
how to configure one touch prov...
what is the site with the most tra...
Previous 7 days
What's new for 20.14?
show in a table
device health
secops dashboard?
What is the health of my network?

You

how to configure custom apps for cloud onramp for saas

AI Assistant

To configure custom apps for Cloud OnRamp for SaaS, you need to define the custom applications using the procedure described in "Define Custom Applications." Then, create an application list with one or more applications, and enable the application list in Cloud OnRamp for SaaS.

You can define custom applications by following the steps in "Create a User-Defined SaaS Application List Using Cisco SD-WAN Manager," which requires a minimum supported release of Cisco IOS XE Catalyst SD-WAN Release 17.8.1a or Cisco vManage Release 20.8.1.

Specifically, you can follow these steps:

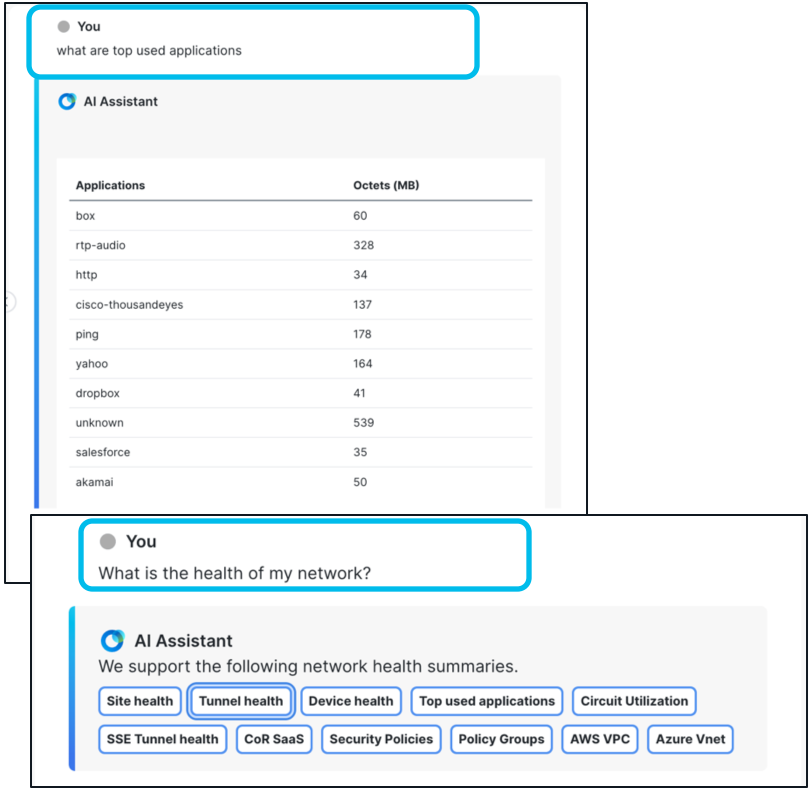
1. Open the Cloud OnRamp for SaaS page using one of the methods described in "Create a User-Defined SaaS Application List Using Cisco SD-WAN Manager."
2. In the Manage Cloud OnRamp for SaaS drop-down list, choose SaaS Application Lists.
3. Click New Custom Application List.
4. Enter a name for the list.
5. To add applications to the list, click the Search field and choose applications. The list includes standard applications and any custom applications that you have defined.
6. Optionally, to create a new custom application within this workflow, click the Search field and then click New Custom Application.

Source:

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/cloudonramp/ios-xe-17/cloud-onramp-book-xe/m-application-lists.html

Assistant can make mistakes. Verify responses.

Use Case: Network Operational Queries



You

what are top used applications

AI Assistant

Applications	Octets (MB)
box	60
rtp-audio	328
http	34
cisco-thousandeyes	137
ping	178
yahoo	164
dropbox	41
unknown	539
salesforce	35
akamai	50

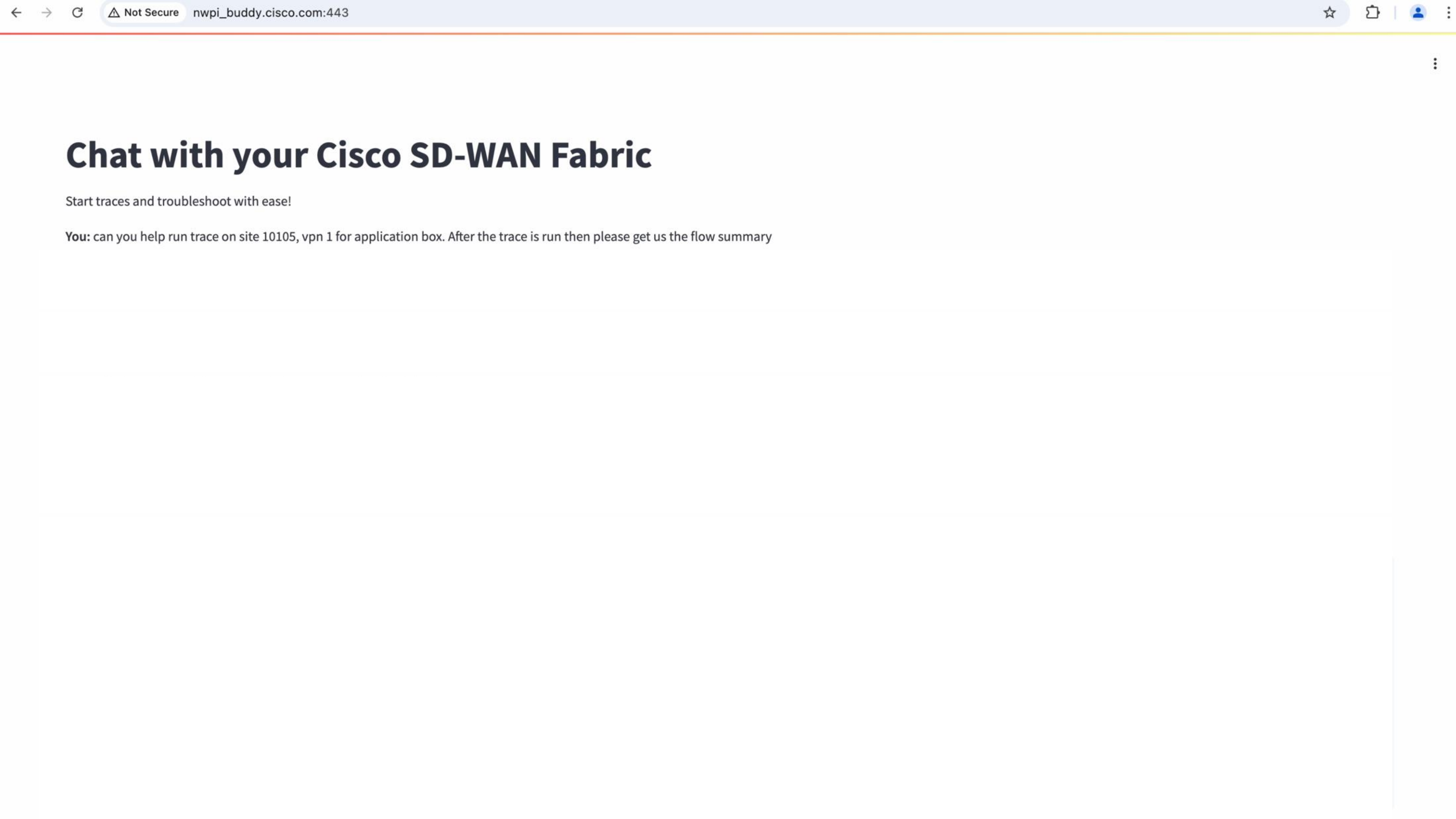
You

What is the health of my network?

AI Assistant

We support the following network health summaries.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Chat with your Cisco SD-WAN Fabric

Start traces and troubleshoot with ease!

You: can you help run trace on site 10105, vpn 1 for application box. After the trace is run then please get us the flow summary

Conclusion

Donnez le Meilleur du SD-WAN à votre entreprise!

- Des fonctionnalités d’IA qui offrent des bénéfices concrets dans la gestion de votre réseau au quotidien
  - Amélioration de l’experience utilisateur
  - Simplification des operations réseau
  - Pouvoir comprendre et optimiser son réseau sans être expert

- Une sécurité intégrée au SD-WAN et aux autres solutions Cisco (Campus/SSE/DC) pour une approche unifiée Zero Trust

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Go Beyond with Cisco CX !

Meet us @World of Solution Booth

	Premium Support		Solution Attached Services		Lifecycle Services
	Service	Case	Service	Use Case	Example Activities
Secure Campus and Branch Networking Get secure networking with real-time performance data, smart recommendations, and closed-loop automation	Success Tracks WAN	Insights to improve, optimize, and secure SD-WAN whether the use case is Secure Automated WAN, Secure Direct Internet Access, or WAN Digital Transformation on ramping for customers migrating from a non-controller environment	SAS SD-WAN	Adoption support for Cisco SD-WAN, Routing, and SASE	Utilize automation capabilities across facets of the network including Catalyst Center SD-WAN with SVS and Services-as-Code to dynamically adjust network configurations based on real-time demand and usage patterns, and AIA (automated incident and assurance) for automated fault detection.

cisco Connect

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

cisco Connect

GO **BEYOND**

#CiscoConnect